Exercice

Cet exercice porte sur l'utilisation des chiffrements symétrique et asymétrique.

Bob souhaite envoyer un message confidentiel à Alice sans qu'un espion, Marley, ne puisse le lire ou le modifier. Pour cela, il envisage plusieurs méthodes de chiffrement et de signature numérique.

Rappel des commandes OpenSSL

Avant de commencer, voici un rappel des principales commandes OpenSSL utilisées pour le chiffrement et la signature numérique.

1. Chiffrement symétrique

Pour chiffrer le fichier `toto.txt` : (un fichier `toto.enc` est alors créé)

```
openssl enc -bf-cbc  -in toto.txt -out toto.enc
```

Pour déchiffrer le fichier `toto.enc` : (un fichier `toto.decode` est alors créé)

```
openssl enc -bf-cbc -d -in toto.enc -out toto.decode
```

3. Chiffrement asymétrique

Pour chiffrer le fichier `toto.txt` avec la clé `KeyPub.pem` : (un fichier `toto.enc` est alors créé)

```
openssl rsautl -encrypt -in toto.txt -inkey KeyPub.pem -pubin -out toto.enc
```

Pour déchiffrer le fichier `toto.enc` avec la clé `Key.pem` (un fichier `toto.decode` est alors créé) :

```
openssl rsautl -decrypt -in toto.enc -inkey Key.pem -out toto.decode
```

4. Signature numérique et vérification

Pour générer une empreinte (avec une fonction de hachage) du document `toto.txt` (un fichier `empreinte.txt` est alors créé)

```
openssl dgst -md5  toto.txt -out empreinte.txt
```

Pour générer une signature à partir du fichier `empreinte.txt` et d'une clé `Key.pem` : (un fichier `signature.txt` est alors créé)

```
openssl rsautl -sign -in empreinte.txt -inkey Key.pem -out signature.txt
```

Pour retrouver l'empreinte à partir de la signature (`signature.txt`) et d'une clé publique `KeyPub.pem` : (un fichier `empreinte1.txt` est alors créé)

```
openssl rsautl -verify -in signature.txt -pubin -inkey KeyPub.pem -out empreinte1.txt
```

Questions

1. Bob envisage d'utiliser un chiffrement symétrique pour sécuriser son message.

a. Bob rédige le `message.txt` et le chiffre avec la commande :

```
openssl enc -bf-cbc -in message.txt -out message.enc
```

puis il envoie le fichier `message.enc` à Alice. Quelle commande OpenSSL, Alice doit t-elle écrire pour déchiffrer le message ?

b. Expliquer pourquoi Alice ne pourra pas déchiffrer le fichier `message.enc`.

c. Citer deux avantages du chiffrement symétrique.

d. Quel est le plus grand inconvénient du chiffrement symétrique ?

2. Afin d'améliorer la sécurité de la communication avec Alice, Bob découvre le chiffrement asymétrique. Bob et Alice ont tous les deux généré une clé publique (`KeyPubAlice.pem` et `KeyPubBob.pem`) et une clé privée (`KeyPrivAlice.pem` et `KeyPrivBob.pem`)

a. Quelle est la différence entre clé privée et clé publique ?

b. Citer un avantage du chiffrement asymétrique.

c. Voici la commande que Bob écrit pour chiffrer le `message.txt` qu'il souhaite transmettre à Alice :

```
openssl rsautl -encrypt -in message.txt -inkey KeyPubliqueBob.pem -pubin -out message.enc
```

Il envoie le fichier `message.enc` à Alice. Expliquer pourquoi Alice n'arrivera pas à déchiffrer le fichier `message.enc`.

d. Bob a enfin réussi à chiffrer correctement : `message.txt` en `message.enc`. Expliquer comment Alice doit procéder pour déchiffrer le message. (On ne demande pas les commandes OpenSSL mais une explication de la démarche)

e. Maintenant Bob souhaite transmettre un diaporama à Alice. Malheureusement, et malgré l'exactitude de la commande OpenSSL utilisé par Bob, le chiffrement asymétrique ne fonctionne pas. Expliquer pourquoi.

f. Bob a compris son erreur et voici les commandes OpenSSL qu'il a tapé pour pouvoir envoyer son diaporama de façon sécurisé :

```
openssl rsautl -encrypt -in password.txt -inkey KeyPubAlice.pem -pubin -out password.enc
openssl enc -bf-cbc -in diaporama.pdf -out diaporama.enc
```

i. Quels sont les fichiers qu'il doit transmettre à Alice ?

ii. Comment Alice va t-elle faire pour déchiffrer le fichier `diaporama.enc` ? (On ne demande pas les commandes OpenSSL mais une explication de la démarche)

3. Bob veut s'assurer que le diaporama qu'il envoie n'est pas altéré et qu'Alice peut vérifier son authenticité. Dans cette partie, on suppose que Alice et Bob ont échangé une clé (ou mot de passe) permettant de communiquer via un chiffrement symétrique.

a. Voici la démarche faite par Bob pour mettre en place cela :

— Il prépare son fichier `diaporama.pdf`.

— Il chiffre son fichier : `diaporama.pdf` avec un chiffrement symétrique :

```
openssl enc -bf-cbc -in diaporama.pdf -out diaporama.enc
```

— Avec une fonction de hachage, il génère une empreinte de son diaporama :

```
openssl dgst -md5 diaporama.pdf  -out empreinte.txt
```

— En utilisant sa clé privée, il génère une signature (`signature.txt`) à partir du fichier `empreinte.txt` :

```
openssl rsautl -sign -in empreinte.txt -inkey KeyPrivBob.pem -out signature.txt
```

Quels sont les fichiers que Bob va transmettre à Alice ?

b. Comment Alice va t-elle faire pour déchiffrer le diaporama et s'assurer qu'il n'a pas été modifié ? (On pourra écrire les commandes OpenSSL ou expliquer la démarche à l'aide de phrases.)

c. Attaque 1 : Marley réussi à se procurer le fichier `signature.txt`, peut-il déchiffrer ce fichier ? Si oui, que dire de son contenu ? si non, expliquer pourquoi ?

d. Attaque 2 : Marley a réussi à se procurer le fichier `diaporama.enc` et a aussi réussi à déchiffrer le fichier `signature.txt`, peut-il alors réussir à déchiffrer le fichier `diaporama.enc` ?

e. Attaque 3 : Marley a réussi à se procurer la clé que Bob et Alice utilise pour le chiffrement symétrique ainsi que le fichier `diaporama.enc`.

i. Marley peut-il déchiffrer le fichier `diaporama.enc` ?

ii. Marley décide alors de remplacer le fichier `diaporama.enc` de Bob et par un nouveau diaporama qu'il nomme aussi `diaporama.enc`. Expliquer comment Alice va s'en rendre compte. (On ne demande par de commande OpenSSL)

f. Attaque 4 : Marley décide non seulement de remplacer le fichier `diaporama.enc` mais aussi de remplacer le fichier `signature.txt` avec les commandes :

```
openssl enc -bf-cbc -in diaporama.pdf -out diaporama.enc
openssl dgst -md5  diaporama.pdf -out empreinte.txt
openssl rsautl -sign -in empreinte.txt -inkey KeyPrivMarley.pem -out signature.txt
```

Expliquer comment Alice va s'en rendre compte. (On ne demande par de commande OpenSSL)

g. Attaque 5 : Proposer une autre idée à Marley afin de réussir à déjouer la sécurité mise en place par Bob et Alice.